UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

CAROL FRAKER, ERICA REYES, BRITTANY MEADOWS, and DAVID CUSTIS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CHANGE HEALTHCARE INC., OPTUM, INC. and UNITEDHEALTH GROUP INCORPORATED,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Carol Fraker, Erica Reyes, Brittany Meadows, and David Custis ("Plaintiffs"), individually and on behalf of all others similarly situated, allege the following based on their personal experience and their counsel's investigation:

INTRODUCTION

1. Plaintiffs brings this proposed class action lawsuit against Defendants Change Healthcare Inc., Optum, Inc., and UnitedHealth Group Incorporated ("Defendants") for their negligent failure to protect Plaintiffs' and Class members' confidential health and personal identifying information from ALPHV/Blackcat ("Blackcat"), a well-known group of cybercriminals. Defendants are key players in the U.S. health industry and together, they process 50% of all medical claims in the United States through a pervasive network of approximately 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals and 600 laboratories.

2. On or around February 21, 2024, Blackcat infiltrated Defendants' information technology networks and then stole for ransom the confidential personal identifying information ("PII") and personal health information ("PHI") of millions of patients across the United States ("Data Breach"). The stolen information includes names, phone numbers, addresses, Social Security Numbers, medical and dental records, insurance records, and claims and payment information, among other things. Blackcat also encrypted portions of Defendants' network, essentially locking them out.

3. In response to the security breach, Defendants immediately took their network systems offline. According to a statement from Change Healthcare, the systems would "remain offline until [they] can be turned back on safely."[1]

4. The Data Breach and shutdown crippled the U.S. healthcare system and has negatively impacted patients, hospital systems, physicians, clinical social workers, and both private and government-owned pharmacies. Medical providers could not verify insurance coverage for patient treatment and procedures or receive reimbursement for services rendered. According to an estimate

[1] *See* https://www.usnews.com/news/health-news/articles/2024-03-04/explainer-what-to-know-about-the-change-healthcare-cyberattack (last visited March 4, 2024).

from First Health Advisory, a digital risk assurance firm, the Data Breach "is costing some providers over $100 million a day."[2]

5. But perhaps the most negatively impacted are patients who cannot timely access medical treatment, including much needed prescription drugs, and now face a significant and increased risk of identity theft. According to Rick Pollack, President and CEO of the American Hospital Association ("AHA"), the Data Breach is the "most serious incident of its kind leveled against a U.S. healthcare organization."

6. Blackcat is known to target organizations with high-value data, such as PHI, and once inside their networks, Blackcat encrypts the organization's data, networks, and servers to block the organization from access until a ransom is paid in exchange for a key that releases the data. But even when Blackcat's demands are met, it may publish the stolen data on the Dark Web. Blackcat affiliates claim they still have the stolen data although a ransom has allegedly been paid by UnitedHealth Group.

7. The U.S. government has warned that Blackhat has hit at least 70 organizations since December 2023, a majority of them healthcare organizations.

8. Plaintiffs, individually and on behalf of all others similarly situated, alleges claims for negligence, negligence *per se*, and unjust enrichment against Defendants and seek all available monetary relief.

PARTIES

9. Carol Fraker is a resident and citizen of Ocean Shores, Washington.

10. Plaintiff Erica Reyes is a resident and citizen of Houston, Texas.

11. Plaintiff Brittany Meadows is a resident and citizen of Jacksonville, Florida.

12. Plaintiff David Custis is a resident and citizen of Shreveport, Louisiana.

13. Defendant Change Healthcare Inc. is a publicly traded company with its principal place

[2] *Id.*

of business in Nashville, Tennessee and is incorporated in Delaware. It became a subsidiary of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UnitedHealth Group subsidiary.

14. Defendant Optum, Inc. ("Optum") maintains its principal place of business in Eden Prairie, Minnesota and is incorporated in Delaware.

15. Defendant UnitedHealth Group Incorporated is one of the largest publicly traded companies by revenue and maintains its principal place of business in Minnetonka, Minnesota and is incorporated in Delaware. UnitedHealth Group exercises control over the management of the Change Healthcare cybersecurity systems as evidenced by UnitedHealth Group's response to the Data Breach as alleged herein.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed class, including Plaintiffs, are citizens of a state different from Defendants. The Court has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

17. This Court may exercise jurisdiction over Defendants because they are registered to conduct business in Tennessee; have sufficient minimum contacts in Tennessee; and intentionally avail themselves of the markets within Tennessee through the promotion, sale, and marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

18. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant Change Healthcare Inc. resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Background

19. Change Healthcare is a healthcare technology company that works across the U.S. health system "to make clinical, administrative and financial processes simpler and more efficient for payers, providers, and consumers." Change Healthcare offers healthcare providers such as doctors, hospitals, therapists, pharmacies, laboratories, and clinics services and support in key areas such as provider claim processing, pharmacy claim transactions, verification of insurance, disbursement of provider payments, and authorizations and medical necessity reviews. Healthcare providers utilize Change Healthcare's services either through a direct contractual relationship or indirectly through third-party intermediaries.

20. According to the Change Healthcare website, its "extensive network, innovative technology, and expertise inspire a stronger, better coordinated, increasingly collaborative, and more efficient healthcare system." It bills itself as a "trusted partner for organizations committed to improving the healthcare system through technology."

21. Change Healthcare also represents to providers that its "advanced technology and services help . . . enhance patient engagement and access, improve outcomes, drive revenue performance, and improve operational efficiency." Change Healthcare represents to payers that its "advanced technology solutions and services help payers achieve their priorities across the member journey." Change Healthcare promises its partners that its "advanced technology solutions empower our partners to achieve their strategic business objectives and meet their customers' needs." And it assures patients that its "solutions streamline the engagement, care, and payment experience to improve the patient journey."

22. Change Healthcare processes 15 billion healthcare transactions annually and touches one in every three U.S. patient records through its clinical connectivity solutions.

23. Previously, Change Healthcare was an independent company that was not owned by any particular healthcare provider or insurer. In 2021, UnitedHealth Group ("UHG") proposed a deal to acquire Change Healthcare for a merger with Optum, a healthcare provider and subsidiary of UHG.

24. Melinda Reid Hatton, AHA Vice President and General Counsel, voiced concerns about the proposed deal and wrote to the Department of Justice ("DOJ") asking it to investigate. In the letter to the DOJ, Ms. Hatton wrote, "The proposed acquisition would produce a massive consolidation of competitively sensitive healthcare data and shift such data from Change Healthcare, a neutral third party, to Optum."

25. The DOJ investigated and filed a complaint to stop UHG's transaction. In its complaint, the DOJ described Change Healthcare as a technology company that operates "the nation's largest electronic data interchange (EDI) clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions . . . It has access to a vast trove of competitively sensitive claims data that flows through its EDI clearinghouse-over a decade's worth of historic data as well as billions of new claims each year."

26. Moreover, according to the DOJ, "50 percent of all medical claims in the United States pass through Change's EDI clearinghouse. Change's self-described 'pervasive network connectivity,' including approximately "900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals and 600 laboratories,' means that even when United's health insurer rivals choose not to be a Change customer, health insurers have no choice but to have their claims data pass through Change's EDI clearinghouse. Not only does Change process vast amounts of competitively sensitive claims data, but it also has secured 'unfettered' rights to use over 60 percent of this data for its own business purposes including, for example, using claims data for healthcare analytics. Additionally, through its claims editing product, Change has access to the proprietary plan and payment rules for all of United's most significant health insurance competitors."

27. The DOJ, however, lost its challenge to UHG's acquisition of Change Healthcare after a district judge ruled in UHG's favor, and the DOJ chose not to appeal.

28. In October 2022, Optum completed its combination with Change Healthcare. According to a press release UHG issued, "The combined businesses share a vision for achieving a simpler, more intelligent and adaptive health system for patients, payers and care providers. The combination will connect and simplify the core clinical, administrative and payment processes

health care providers and payers depend on to serve patients. Increasing efficiency and reducing friction will benefit the entire health system, resulting in lower costs and a better experience for all stakeholders."

Defendants are Targeted for Their Treasure Trove of Health Data

29. On February 21, 2024, Defendants discovered the Data Breach and that their computer networks were not secure and could not protect PHI and PII as required by state and federal law. UHG set up a website regarding the Data Breach at www.unitedhealthgroup.com to announce the Data Breach and stated that it disconnected the Change Healthcare systems. UHG made a similar statement in a filing with the U.S. Securities and Exchange Commission. UHG also stated, "The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies . . . At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational."

30. In a public statement, Defendants stated:

> Change Healthcare can confirm we are experiencing cyber security issues perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat.
>
> Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants, Mandiant and Palo Alto Network, on this attack against Change Healthcare's systems. We are actively working to understand the impact to members, patients, and consultants.
>
> Patient care is our top priority, and we have multiple workarounds to ensure people have access to the medications and the care they need. Based on our ongoing investigation, there's no indication that Optum, UnitedHealthcare and UnitedHealthcare Group systems have been affected by this issue.
>
> We are working on multiple approaches to restore the impacted environment and continue to be proactive and aggressive with all our systems, and if we suspect any issue with the system, we will immediately take action.[3]

[3] *See* https://status.changehealthcare.com/incidents/hqpjz25fn3n7 (last visited March 4, 2024)

31. Upon the public announcement, the AHA issued a security advisory on February 22, 2024, stating:

> Due to the sector wide presence and the concentration of mission critical services provided by Optum, the reported interruption could have significant cascading and disruptive effects on revenue cycle, certain health care technologies and clinical authorizations provided by Optum across the health care sector. Based upon the statements from Change Healthcare that they became aware of an "outside threat" and disconnected "in the interest of protecting our partners and patients," **we recommend that all health care organizations that were disrupted or are potentially exposed by this incident consider disconnection from Optum until it is independently deemed safe to reconnect to Optum**. It also is recommended that organizations which utilize Optum's services prepare related downtime procedures and contingency plans should Optum's services remain unavailable for an extended period.[4]

(emphasis in original).

32. Two days later, AHA issued another security advisory notifying members and the public that "**Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected**" (emphasis in original).[5] The AHA also recognized that hospitals and health systems "may be experiencing challenges with obtaining care authorizations for their patients, as well as delays in payment."[6] It stated that it was in communication with the Department of Health and Human Services, including the Centers for Medicare & Medicaid Services, about "options to support patients' timely access to care and provide temporary financial support to providers. We also are having these discussions with Optum. We will provide more information as it becomes available."[7]

---

[4] *See* https://www.aha.org/advisory/2024-02-22-unitedhealth-groups-change-healthcare-experiencing-cyberattack-could-impact-health-care-providers-and (last visited March 4, 2024).

[5] *See* https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers (last visited March 4, 2024).

[6] *Id.*

[7] *Id.*

33. On February 23, 2024, the AHA called the Data Breach a "threat to life," and in a letter to Health and Human Services, the AHA stated that while the full scope was "unknown," the AHA expected impacts to be far-reaching given Change Healthcare's national presence.[8] The AHA also explained how the incident has affected healthcare providers in terms of being unable to collect revenue. "[W]ithout this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services," the AHA stated.[9] "In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks. It is particularly concerning that while Change Healthcare's systems remain disconnected, it and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers."[10]

34. Antitrust experts have opined that the Data Breach shows why placing "one conglomerate at the center of multiple health care functions is inherently risky."[11]

The Change Healthcare Data Breach Cripples the Healthcare Industry

35. The Data Breach at Change Healthcare has had reverberations across the U.S. healthcare industry that continue today. The most negatively impacted are patients who have had trouble accessing their prescriptions and healthcare and now face an increased risk of identity theft.

36. One week after the Data Breach, hospitals, healthcare providers, and pharmacies across the U.S. reported that they were unable to process and fill prescriptions through patients' insurance.

---

[8] *See* https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack (last visited March 4, 2024).

[9] *Id.*

[10] *Id.*

[11] *See* https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/ (last visited March 4, 2024).

37. U.S. military insurance provider, Tricare, said that the Data Breach was "impacting all military pharmacies worldwide and some retail pharmacies nationally."[12]

38. In a post on X, the Naval Hospital in Camp Pendleton, California said it was unable to process any prescriptions.[13] "Due to an ongoing enterprise-wide issue, all Camp Pendleton and associated pharmacies are unable to process any prescription claims," Camp Pendleton said.[14] "As a result, we are only able to assist patients with emergency and urgent prescriptions from hospital providers at this time."[15]

39. In a Facebook post, Evans Army Community Hospital similarly reported problems: "This outage is impacting dispensing of pharmacy prescriptions – resulting in delays in processing and in some cases, inability to process. Refills have also been impacted."[16]

40. GoodRx, which offers discounted prescriptions, also said on X: "We apologize for any outages you have been experiencing while at the pharmacy . . . Unfortunately, the issue is an external one impacting both GoodRx and a multitude of providers."[17]

41. Large pharmacy chains like CVS and Walgreens have also reported disruptions as well as smaller ones like Moffet Drug in Norton, Kansas.[18]

42. Armish Patel, a pharmacist in Dallas, Texas, told CBS: "So I mean we've seen a lot of claims coming through as a rejected claim, where obviously the insurance provider are

---

[12] *See* https://tcrn.ch/3Tg4jsV (last visited March 4, 2024).

[13] *See* https://www.cnn.com/2024/02/22/tech/us-pharmacies-face-delays-filling-prescriptions-because-of-cyberattack/index.html (last visited March 4, 2024).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *See* https://www.cnn.com/2024/02/22/tech/us-pharmacies-face-delays-filling-prescriptions-because-of-cyberattack/index.html (last visited March 4, 2024).

not able to pay because of this attack . . . Elderly patients that have a fixed income, and they're trying to get their medicine…unfortunately there's no way around it at this point."[19]

43. One consumer, Cary Brazeman, told CNBC that he tried to pick up a prescription at Vons pharmacy in Palm Springs after seeing his dermatologist but was told by the pharmacy that it had not received his prescription and that even if it had, it would not have been able to process it with his insurance. Brazeman asked what he was supposed to do, and was told by the pharmacy, "We don't know." Brazeman told CNBC, "I'm mobile, so I can make the rounds if necessary, and I can pay cash if necessary, but there's a lot of people who cannot."[20]

44. The fallout from the Data Breach has also impacted medical care providers, both large and small.

45. A majority of Nebraska hospitals have also been unable to verify patient insurance, process billing, or provide accurate cost estimates, according to Nebraska television outlet KLKN-TV.[21] When insurance cannot be verified, treatment is delayed.

46. Similarly, independent medical practitioners reported to CNBC that they also have been unable to verify patients' eligibility for patients or electronically fill prescriptions, which has created a headache and more clerical work that is overwhelming and time consuming.[22]

47. Moreover, some medical practices, especially smaller ones and mid-sized offices, rely on cash flow from claims reimbursements that are not being processed. Dr. Purvi Parikh told CNBC that her practice has not been paid from insurers for her patients' visits, which creates

---

[19] *See* https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/ (last visited March 4, 2024).

[20] *See* https://www.cnbc.com/2024/02/27/unitedhealths-change-healthcare-cyberattack-outages-continue-pharmacies-deploy-workarounds.html (last visited March 4, 2024).

[21] *See* https://tcrn.ch/3Tg4jsV (last visited March 4, 2024).

[22] *See* https://www.nbcnews.com/news/us-news/outages-change-healthcare-cyberattack-causing-financial-mess-doctors-rcna141321 (last visited March 4, 2024).

problems for paying operational expenses like medical supplies and payroll.[23] Dr. Parikh said there were no immediate workarounds and that it could take weeks to change to a new platform.[24]

48. Licensed clinical social worker Jenna Wolfson reported that she has been unable to receive any payments due to the Change Healthcare Data Breach and that many of her colleagues are facing the same problems.[25] According to Wolfson, "There are people right now that might not see payment on the work that they're doing today for months, and they still have an entire practice to keep above water."[26]

The Data Breach Placed the Confidential Health and Personal Identifying Information of Patients at Risk

49. UHG initially claimed that a nation-state actor was responsible for the Data Breach. Blackcat, however, claimed responsibility and stated on its dark web leak site that it had stolen the confidential health and personal identifying information relating to millions of Americans.

50. Specifically, Blackcat said it gained access to 6TB of data, including medical records, and payment and claims information containing personally identifiable information like names, contact information such as phone numbers and email addresses, and Social Security Numbers.

51. Blackcat also claims to have Change Healthcare's source code and confidential and sensitive information of CVS Caremark, Metlife, Health Net, Federal Medicare, and Tricare.

52. Below is the statement that Blackcat issued regarding the cyberattack, indicating that the group has reviewed a substantial amount of confidential medical and personal identifying information:

Change Healthcare - Optum - UnitedHealth

2/28/2024, 4:19:59 PM

---

[23] *Id.*

[24] *Id.*

[25] *See* https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-cyberattack-on-providers (last visited March 4, 2024).

[26] *Id.*

UnitedHealth has announced that the attack is "strictly related" to Change Healthcare only and it was initially attributed to a nation state actor.

Two lies in one sentence.

Only after threatning [sic] them to announce it was us, they started telling a different story.

It is true that the attack is centered at Change Healthcare production and corporate networks, but why is the damage extremely high? Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers, insurance providers, pharmacies, etc . . .

Also, being inside a production network one can imagine the amount of critical and sensitive data that can be found.

We were able to exfiltrate to be exact more than 6 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

Anyone with some decent critical thinking will understand what damage can be done with such intimate data on the affected clients of UnitedHealth/UnitedHealth solutions as well, beyond simple scamming/spamming.

After 8 days and Change Health have [sic] still not restored its operations and chose to play a very risky game hence our announcement today.

So for everyone, both those affected and fellow associates. [sic] to understand what is at stake our exfiltrated data includes millions of:

- active US military/navy personnel PII

- medical records
- dental records
- payments information
- Claims information
- Patients PII including Phone numbers/addresses/SSN/emails/etc ...
- 3000+ source code files for Change Health solutions (for source-code review gents out there)
- Insurance records
- many many more

UnitedHealth you are walking on a very thin line be careful you just might fall over.

PS: For all those cyber intelligence so called expert . . . we did not use ConnectWise exploit as our initial access so you should base your reports you tell people on actual facts not kiddi [sic] speculations.

53. On February 28, 2024, UHG confirmed that the Data Breach was perpetrated by Blackcat, which has a history of targeting organizations in the healthcare industry.

54. As a result of the Data Breach, Plaintiffs and the proposed Class have not only lost their privacy, but they are at a significant and increased risk of identity theft.

55. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

56. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and

credit in a person's name.[27] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

57. Accordingly, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[28]

58. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

59. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[46]

60. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

61. For all of the above reasons, Plaintiffs and the Class members have suffered harm and there is a substantial risk of injury to them that is imminent and concrete and that will continue for years to come.

---

[27] *See* Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown (June 2007), United States Government Accountability Office, available at https://www.gao.gov/new.items/d07737.pdf (last accessed March 4, 2024).

[28] Guide for Assisting Identity Theft Victims, Federal Trade Commission, 4 (September 2013), available at http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last accessed March 4, 2024).

[29] GAO Report at 29.

The Data Breach was a Foreseeable Risk of Which Defendants were on Notice and Could Have Prevented

62. The healthcare industry is the most targeted industry by cybercriminals; cyberattacks have doubled from 2016 to 2021. As a result, the personal health information of approximately 42 million patients has been exposed.[30]

63. Identity thieves and cybercriminals have targeted the medical industry in the last several years given the treasure trove of ultra-sensitive personal data stored on their systems. The medical industry is rife with examples of cybercriminals targeting healthcare providers.

64. In addition, cyberattacks at medical facilities wreak havoc on patients' lives because they disrupt the medical treatments needed, resulting in delays or cancellations in receiving medical care. Such attacks cause loss of access to patient medical records, including charts, x-rays, and other information needed to treat patients.

65. The Department of Health and Human Services in 2017 released a ransomware fact sheet advising entities covered by HIPPA that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule."

66. Under the HIPAA Privacy Rules, a breach is defined as, ". . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." Accordingly, attacks like the one at issue are considered a breach under the HIPPA Rules because there was an access of PHI not permitted under the HIPPA Privacy Rule.

67. A ransomware attack is also considered a "Security Incident" under HIPPA.

---

[30] *See* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9856685/#:~:text=In%20this%20cohort%20study%20of,of%20nearly%2042%20million%20patients (last visited March 4, 2024).

Under the HIPPA Rules, a "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." According to the Department of Health and Human Services, "[t]he presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule."

68. As early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

69. Data Breaches can be prevented. Approximately 80% of ransomware is delivered through email phishing attacks. Other means to deliver ransomware is through brute force attacks on open remote desktop protocol ports. To prevent ransomware attacks, organizations must provide training to its employees for the handling of suspicious emails. They can also disable macros, avoid storing passwords in plain text, and perform hunts and search for suspicious behavior in their networks, among other things.

70. Accordingly, Defendants knew, given the vast amount of PII and PHI they acquire, manage and maintain, that they were a target of security threats, and therefore understood the risks posed by their insecure data security practices and systems. Defendants' failure to heed warnings and to otherwise maintain adequate security practices resulted in this ransomware attack.

Defendants, at all Relevant Times, had a Duty to Plaintiffs and Class Members to Properly Secure Their PII and PHI

71. Defendants, at all relevant times, had a duty to Plaintiffs and Class members to properly secure their PII and PHI, encrypt and maintain such information using industry standard methods, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harms to Plaintiffs and Class members, and promptly notify patients when Defendants became aware that patients' PII and PHI was compromised.

72. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them, on the one hand, and Plaintiffs and the other Class

members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted Defendants (or their providers who entrusted Defendants) with their PII and PHI as part of receiving or paying for medical services and prescription drugs. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligations to protect such information. Accordingly, Defendants breached its common law, statutory and other owed duties to Plaintiffs and Class members.

73. Defendants' duty to use reasonable security measures also arose under HIPAA. Defendants are covered by HIPAA and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. Under HIPAA, Defendants were required to "reasonably protect" PHI from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

74. Under HIPPA, Defendants were also required to do the following:

- Ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted. 45 C.F.R. § 164.306(a)(1);
- Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);
- Implement policies and procedures to prevent detect, contain, and correct security violations. 45 C.F.R. § 164.308(a)(1)(i);
- Implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D);

- Protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI. 45 C.F.R. § 164.306(a)(2);
- Protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information. 45 C.F.R. § 164.306(a)(3);
- Ensure compliance with HIPAA security standard rules by its workforces. 45 C.F.R. § 164.306(a)(4);
- Train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); and/or
- Render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304 definition of encryption).

75. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendant.

76. The Data Breach was a direct and proximate result of Defendants' failure to: (1) properly safeguard and protect Plaintiffs' and Class members' PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII and PHI; and (3) protect against reasonably foreseeable threats to the security or integrity of such information.

Plaintiffs' Experiences

77. Plaintiff Carol Fraker has a medical condition that requires that she use certain medications every day. Plaintiff Carol Fraker uses a discount card issued by Eli Lilly for her monthly supply prescriptions. She uses AmeriPharma to fill her prescriptions. Her prescription requires a once-a-week injection.

78. On or around February 28, 2024, Plaintiff Fraker tried to fill her prescription using her discount card at AmeriPharma, but AmeriPharma was unable to process her discount card. Plaintiff Fraker was told that AmeriPharma could not fill her prescription because systems were down since February 21, 2024, and they did not know when the systems would be fixed.

79. Since she was not able to get her prescription filled, she had to use a different class of medication that required injections three times a day as opposed to a once a week injection.

80. On or about March 25, 2024, through her own research and efforts, Plaintiff Fraker learned that Eli Lilly offered a new discount card to address issues caused by the Data Breach and shutdown; and was able to get her prescription filled with her new discount card for $25.00.

81. Plaintiff Fraker also has spent time and efforts researching the data breach and reviewing her financial information to determine if there has been unauthorized activity to her accounts and will perform these activities for the foreseeable future. In addition to not being able to timely obtain her necessary medication, Plaintiff Fraker has suffered emotional distress due to the data breach and concerns that her PII and PHI is in the hands of cybercriminals and can be ransomed again and otherwise used for identity theft.

82. Plaintiff Erica Reyes has a medical condition that requires that she take certain medications every day. She uses a specialty pharmacy, Lumicera, to fill her prescriptions.

83. On February 21, 2024, Plaintiff Reyes tried to fill her prescriptions and needed them by February 22, 2024, to treat her medical condition. Plaintiff Reyes was told that Lumicera could not fill her prescriptions because systems were down. Plaintiff Reyes checked on her prescriptions with Lumicera again on February 22, 2024, and was told that systems were still down. Plaintiff Reyes did not receive her prescriptions until February 26, 2024.

84. Plaintiff Reyes has spent time and efforts researching the data breach and reviewing her financial information to determine if there has been unauthorized activity to her accounts and

will perform these activities for the foreseeable future. In addition to not being able to timely obtain her necessary medications, Plaintiff Reyes has suffered emotional distress due to the data breach and concerns that her PII and PHI is in the hands of cybercriminals and can be ransomed again and otherwise used for identity theft.

85. Plaintiff Brittany Meadows uses a discount card through AbbVie's co-pay assistance program for her prescriptions. She generally uses Capsule Pharmacy ("Capsule") to fill her prescriptions.

86. On or about February 26, 2024, Plaintiff Meadows tried to fill her prescription using her discount card at Capsule, but Capsule was unable to process her discount card. On or about March 1, 2024, Plaintiff Meadows received a notice from Capsule informing her that the systems were down.

87. On or about March 10, 2024, Plaintiff Meadows tried again to fill her prescription using her discount card with a different pharmacy, Publix Pharmacy ("Publix"), however, Publix, was also unable to process her discount card. Plaintiff Meadows had no alternative options but to pay $166.00 to receive her prescription that day, as opposed to paying $25.00.

88. Plaintiff Meadows has spent time and efforts researching the data breach and reviewing her financial information to determine if there has been unauthorized activity to her accounts and will perform these activities for the foreseeable future. In addition to not being able to timely obtain her prescription, Plaintiff Meadows has suffered emotional distress due to the data breach and concerns that her PII and PHI is in the hands of cybercriminals and can be ransomed again and otherwise used for identity theft.

89. Plaintiff David Custis has a medical condition that requires that he take certain medications every day. Plaintiff Custis uses a discount card. He uses different pharmacies to fill his prescriptions.

90. On or about February 28, 2024, Plaintiff Custis tried to fill his prescription using his discount card at Savon Pharmacy but Savon Pharmacy was unable to process his discount card because systems were down. On or about March 7, 2024, Plaintiff Custis tried again to fill his

prescription using his discount card at a Target Pharmacy, but Target Pharmacy was also unable to process his discount card because systems were down.

91. Plaintiff Custis then tried to fill his prescription at Savon Pharmacy using his discount card, but Savon Pharmacy was unable to process his discount card because systems were down, and Plaintiff Custis had no alternative options but to pay $150.00 to receive his prescription that day, as opposed to paying $25.00.

92. Plaintiff Custis has spent time and efforts researching the data breach and reviewing his financial information to determine if there has been unauthorized activity to his accounts and will perform these activities for the foreseeable future. In addition to not being able to timely obtain his prescription, Plaintiff Custis has suffered emotional distress due to the data breach and concerns that his PII and PHI is in the hands of cybercriminals and can be ransomed again and otherwise used for identity theft.

CLASS ACTION ALLEGATIONS

93. Plaintiffs bring this action individually and on behalf of all other persons similarly situated (the "Nationwide Class") pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4).

94. The Nationwide Class is initially defined as follows: All persons residing in the United States and whose PII and PHI was compromised in the Data Breach announced by Defendants on or around February 21, 2024.

95. Excluded from the proposed Class are: Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

96. Plaintiffs reserve the right to re-define the Class definition after conducting discovery.

97. **Numerosity (Fed. R. Civ. P. 23(a)(1).** The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes millions of

patients who had their PII and PHI compromised. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

98. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)).** Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but not limited to the following:

a. Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs' and Class members' PII and PHI;

b. Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs' and Class members' PII and PHI;

c. Whether Defendants' conduct, practices, actions, and omissions, resulted in or was the proximate cause of the Data Breach, resulting in the loss of PII and PHI of Plaintiffs and Class members;

d. Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and Class members;

e. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

f. Whether and when Defendants knew or should have known that their systems were vulnerable to attack;

g. Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their PII and PHI; and

h. Whether Plaintiffs and Class members are entitled to relief, including damages and equitable relief.

99. **Typicality (Fed. R. Civ. P. 23(a)(3))**. Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the Class members. Plaintiffs, like all Class members, had their PII and PHI compromised in the Data Breach and are at an increased risk of harm, including identity theft.

100. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)**. Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs have retained counsel experienced in prosecuting class actions and data breach cases.

101. **Superiority (Fed. R. Civ. P. 23(b)(3)**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

102. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class members which would establish incompatible standards of conduct for Defendants; or

b. the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to individual Class members which would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

103. **Issue Certification (Fed. R. Civ. P. 23(c)(4).** In the alternative, the common questions of fact and law, set forth in Paragraph 98, are appropriate for issue certification on behalf of the proposed Class.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

104. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

105. Defendants had (and continue to have) a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII and PHI. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of PII and PHI within their possession, custody and control).

106. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and Plaintiffs and Class members, which is recognized by laws including but not limited to HIPAA. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiffs and the Class members from a data breach.

107. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to them - including Plaintiffs' and Class members' PII and PHI. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII and PHI by failing to design,

adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII and PHI.

108. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiffs and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII and PHI within their possession, custody and control.

109. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiffs and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII and PHI.

110. But for Defendant's negligent breach of the above-described duties owed to Plaintiffs and Class members, their PII and PHI would not have been released, disclosed, and/or disseminated without their authorization.

111. Plaintiffs' and Class members' PII and PHI was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and/or disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' PII and PHI.

112. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this ransomware attack constitute negligence.

113. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the ransomware attack, Plaintiffs and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in

monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

114. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

115. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PHI.

116. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

117. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII and PHI.

118. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' PII and PHI.

119. Defendants breached their duties to Plaintiffs and Class Members under HIPAA, the Federal Trade Commission Act, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII and PHI.

120. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

121. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

122. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

123. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

124. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

125. Plaintiffs' and Class members' PII and PHI has value that was conferred on Defendants. Moreover, Plaintiffs and Class members conferred benefits on Defendants in the form of payments for medical and healthcare services, both directly and indirectly. Defendants had knowledge of the benefits conferred by Plaintiffs and Class members and appreciated such benefits. Defendants should have used, in part, the monies Plaintiffs and Class members paid to it, directly and indirectly, to pay the costs of reasonable data privacy and security practices and procedures.

126. Additionally, Defendants utilized Plaintiffs' and Class members' valuable PII and PHI for their own business purposes and because Plaintiffs and Class members bestowed actual

value on Defendants, Defendants were obligated to devote sufficient resources to implement reasonable data privacy and security practices and procedures.

127. Plaintiffs and Class members have suffered actual damages and harm as a result of Defendants' conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received from Plaintiffs and Class members, including damages equaling the difference in value between the medical and healthcare services that included the reasonable data privacy and security practices and procedures Plaintiffs and Class members paid for and the medical and healthcare services without the reasonable data privacy and security practices they actually received.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the members of the Class defined above, respectfully request that this Court enter:

(a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiffs as the Class representatives, and appoint the undersigned as Class counsel;

(b) A judgment awarding Plaintiffs and Class members appropriate monetary relief, including actual damages, statutory damages, punitive damages, equitable relief, restitution, and disgorgement;

(c) An order entering injunctive and declaratory relief as appropriate under the applicable law;

(d) An order awarding Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

(e) An order awarding reasonable attorneys' fees and costs as permitted by law; and

(f) Any and all other and further relief as may be just and proper.

//

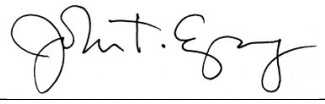
//

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial.

Dated: April 3, 2024

SPRAGENS LAW PLC



John T. Spragens (TN No. 31445)
311 22nd Ave. N.
Nashville, TN 37203
Telephone: (615) 983-8900
Facsimile: (615) 682-8533
john@spragenslaw.com

GIBBS LAW GROUP LLP
Rosemary M. Rivas
David M. Berger
Rosanne L. Mah
1111 Broadway, Suite 2100
Oakland, California 94607
(510) 350-9700 (tel.)
(510) 350-9701 (fax)
rmr@classlawgroup.com
dmb@classlawgroup.com
rlm@classlawgroup.com

Attorneys for Plaintiffs